FortiAuthenticator™ 3.2
What's New Guide

FortiAuthenticator™ 3.2 What's New Guide

October 21, 2014

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2014-10-20	Initial Release

Introduction

This document lists and describes many of the new features added to FortiAuthenticator 3.2. For a complete list of all new FortiAuthenticator 3.2 features and bug fixes, please see the latest release notes.

This document, and all of the FortiAuthenticator 3.2 documentation, will continue to improve as we see the new features in action and as we get feedback about these documents from you. You can send comments and suggestions for improvements for all FortiAuthenticator 3.2 documents to techdoc@fortinet.com.

What's New

FortiAuthenticator 3.2 is a major feature release and includes new features in all functional areas of the product.

System features

These are features related to general system operation and not a specific functional area.

Hyper-V support

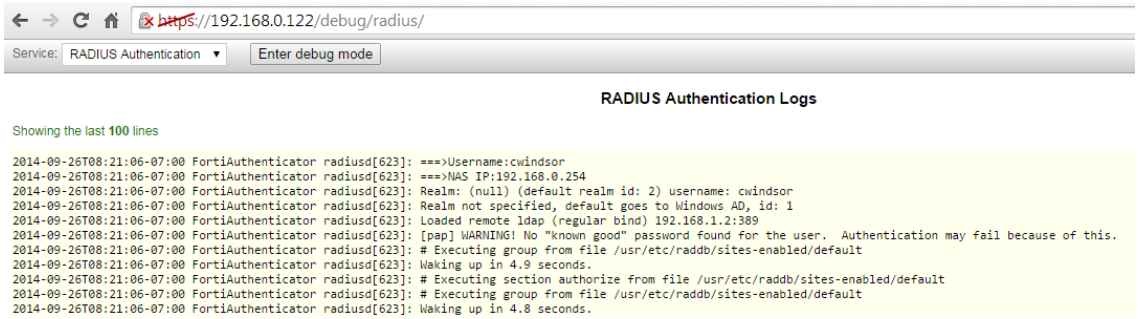
Continuing the Fortinet strategy to support multiple virtual machine hypervisor options, FortiAuthenticator introduces FortiAuthenticator for Hyper-V. This release supports Hyper-V Server 2012 R2 and Hyper-V on Windows Server 2012 R2. Earlier versions may be functional but have not yet been verified and are therefore unsupported. The release notes will be updated as this changes.

Authentication

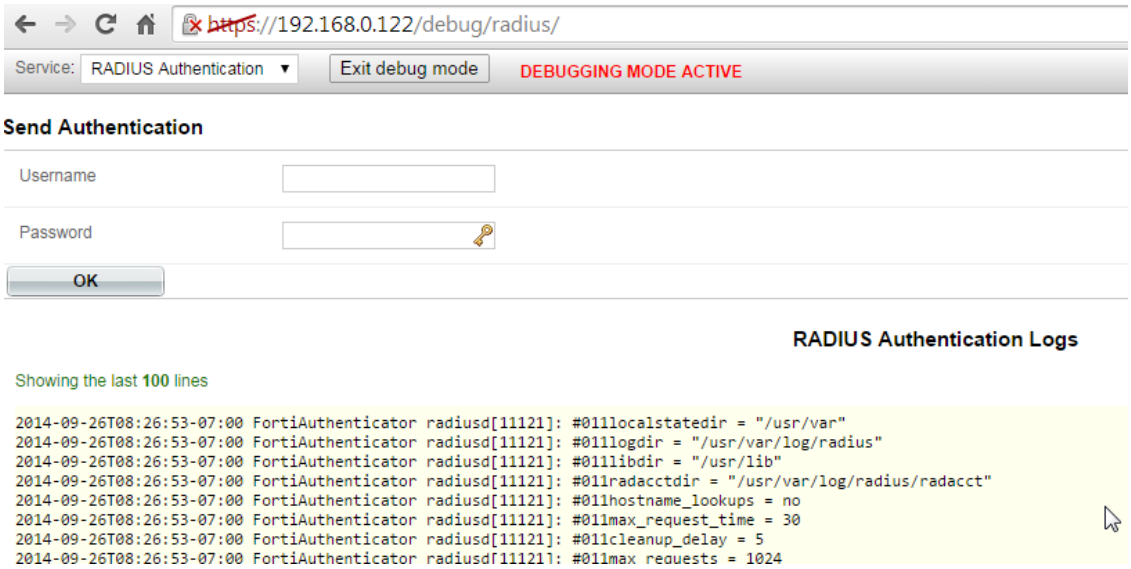
Authentication covers all of the explicit authentication options within the FortiAuthenticator including RADIUS, LDAP, Two-Factor, Tokens, EAP, guest management and user self-service features.

Enhance RADIUS auth debugging

Extended RADIUS debugging can now be enabled by selecting Enter Debug Mode on the debug log page. This enabled verbose logging of the RADIUS daemon.

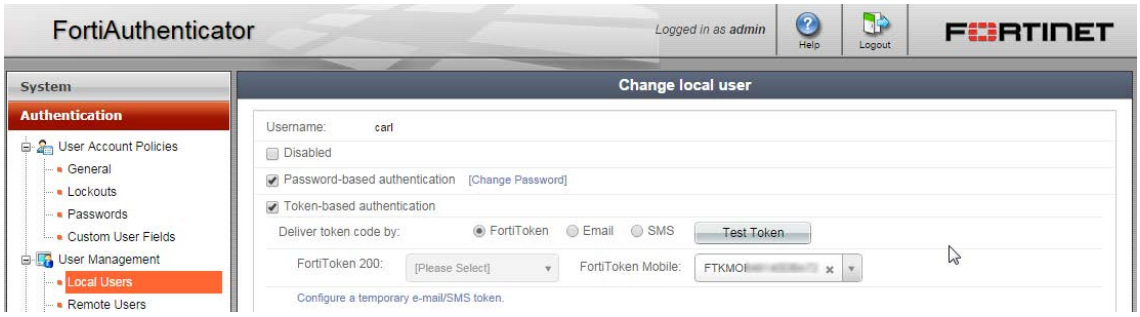


Once enabled, verbose logging will be printed and a new user authentication validation option enabled.



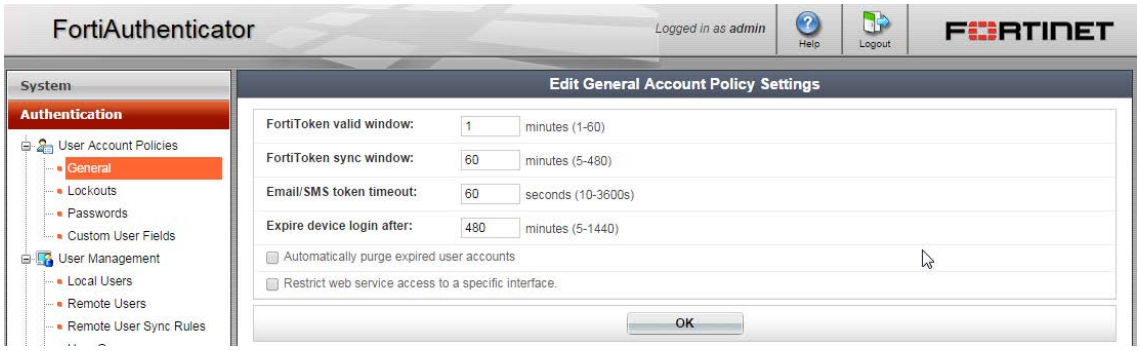
Validate token passcodes

To aid in the debugging of token authentication synchronization issues, a new feature has been added to the user GUI to allow an administrator to validate a user token passcode. This will prove that a token is correctly synchronized and in the position of the correct user. Note that the token remains 'one-time' so the token passcode will not be re-usable and the user must wait for a new code before attempting a subsequent authentication.



Configurable token validation window

To adhere to the OATH Validation Server standard, FortiAuthenticator has introduced the ability to configure the token validation window i.e. the amount of time for either side of the current time for which a token will be considered valid. The default is +/- 1 minute but this can be extended to 60 minutes. Whilst this is possible, the security implication of changing this setting should be carefully considered. RFC6238 recommends the validity window should be set to at most, the same value as one time step i.e. 60s in the case of the FTK200, which is our default.



API auth enhancement

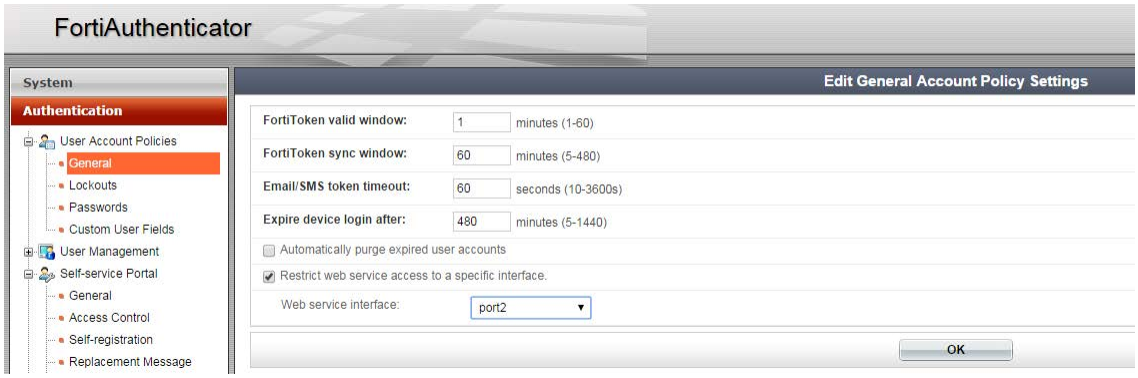
The API has been enhanced to enable several new field requested features:

- Triggering of an Email/SMS token is now supported in `/auth` API
    - Both `/localusers` and `/ldapusers` APIs are extended so that out-of-band token code (for email and SMS tokens) can be sent using the new `/sendoobtoken` resource
- Add `/ldapusers` API with a read-only access, to view user's token-based authentication configuration
- The `/localusers` API now returns an empty string (instead of null) for `token_type` field when user has no token-based authentication configured
- New filter expressions are added to `/localusers` and `/fgtgroupfilter` including `contains, icontains` and `in`

These changes will be documented fully as part of the REST API Guide on http://docs.fortinet.com/fortiauthenticator/admin-guides.

Restrict REST API to specific interface

For security reasons, the REST API can be restricted to specific interfaces.



Windows agent for Microsoft IIS

To enable two-factor authentication to Microsoft Internet Information Services (IIS) based systems, including Microsoft Outlook Web Access (OWA), a new agent has been developed to extend the authentication process with a second factor (token). This will be documented in detail in the Microsoft IIS Agent User Guide on http://docs.fortinet.com/fortiauthenticator/admin-guides.

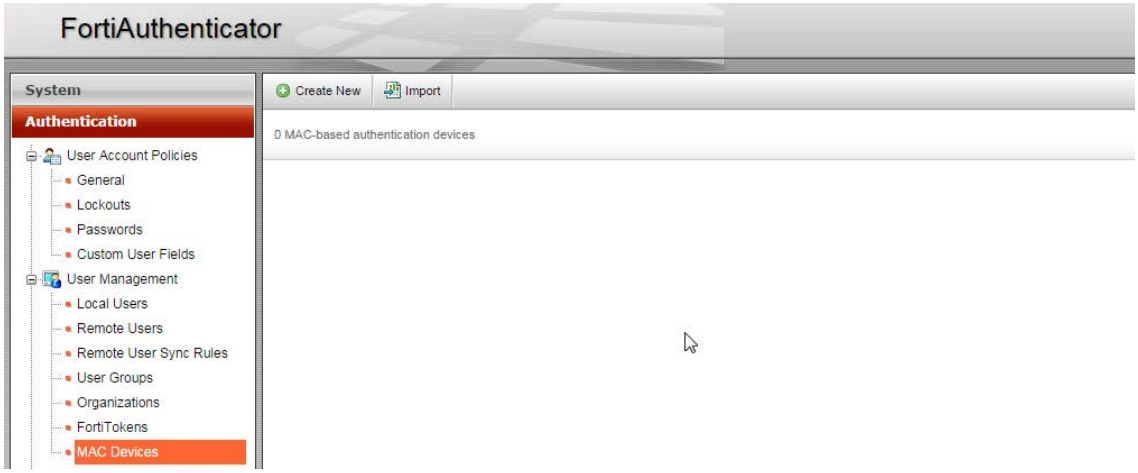
Tested platforms include:

- Microsoft Windows 2012 R2 Server / Microsoft Exchange 2013 (confirmed)
- IIS 7.0 minimum (Vista / Server 2008 and later) (confirmed)
- Microsoft Exchange 2007 / 2010 (in testing)

Note Microsoft Exchange 2003 and earlier are not supported.

Bulk import for MAC devices

To simplify configuration of the MAC Devices feature, importing of a CSV file containing bulk list of MAC addresses is now supported. The supported CSV format is Device name (50 Chars), MAC Address (01:23:45:67:89:ab, or 0123456789AB)



FSSO

Configurable DNS Lookup Options

The following configurable DNS lookup options have been added.

Under *SSO->General->Enable Windows Active Directory domain controller polling*:

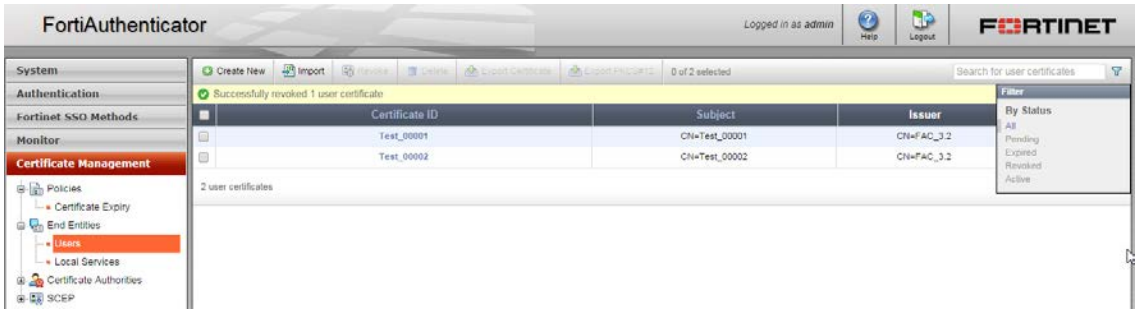
- Enable DNS lookup to get IP from workstation name (default: true)
- Directly use domain DNS suffix in lookup (default: false)
- Enable reverse DNS lookup to get workstation name from IP (default: true)
- Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name (default; false)

The last option is useful when some event contains only IP information, and reverse DNS lookup is used to get the workstation name. After that, the workstation name is used in DNS lookup again to get more complete IP information. This is useful in some environment where workstations have multiple network interfaces.

Certificate Management

Filter options for revoked certificates

On a FortiAuthenticator with many users and the usual level of certificate revocations, it quickly became difficult to browse the certificate GUI. The ability to apply a GUI filter has been added to allow all or pending, expired, active or revoked certificates to be displayed.



Support Extended Attributes

Some certificate use requires the explicit presence of extended key usage attribute before the certificate will be accepted for use. This is particularly true for VPN use on Windows 8.1 mobile devices. FortiAuthenticator adds this functionality during the certificate creation process.